(12) UK Patent Application (19) GB (11) 2 304 077 (13) A

(43) Date of A Publication 12.03.1997

(21) Application No 9525734.1

(22) Date of Filing 15.12.1995

(30) Priority Data
(31) 9513361 (32) 30.06.1995 (33) GB

(71) Applicant(s)
Andrew John Farrall
6 Briar Mead, Yatton, BRISTOL, BS19 4RE,
United Kingdom

(72) Inventor(s)
Andrew John Farrall

(74) Agent and/or Address for Service
Andrew John Farrall
6 Briar Mead, Yatton, BRISTOL, BS19 4RE,
United Kingdom

(51) INT CL[6]
B42D 15/10 , G06K 19/14 // B42D 105:00 205:00

(52) UK CL (Edition O)
B6A AC72 AC81 ATC
G4M MB4 MCA
U1S S2271 S2272 S2273 S2291

(56) Documents Cited
EP 0570162 A2 EP 0388713 A2 EP 0364029 A1
EP 0230497 A1 US 4423415 A US 4218674 A

(58) Field of Search
UK CL (Edition O) B6A ATC
INT CL[6] B42D 15/00 15/10 , G06K 19/06 19/14 , G07F 7/08
Online databases: WPI

(54) Security device comprising reflective particles

(57) A security device comprises reflective particles in the form of flakes or granules 50 randomly distributed in three dimensions throughout the substrate 10 or in a coating 53. The particles reflect light at different angles and directions thereby creating a unique reflected light signature for detection by a reading device. The flakes may be of metal. The device may be a credit card or identity card, tag or label.

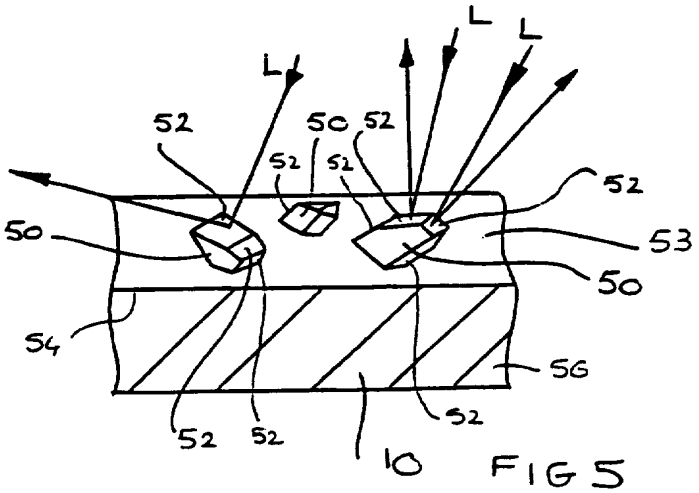
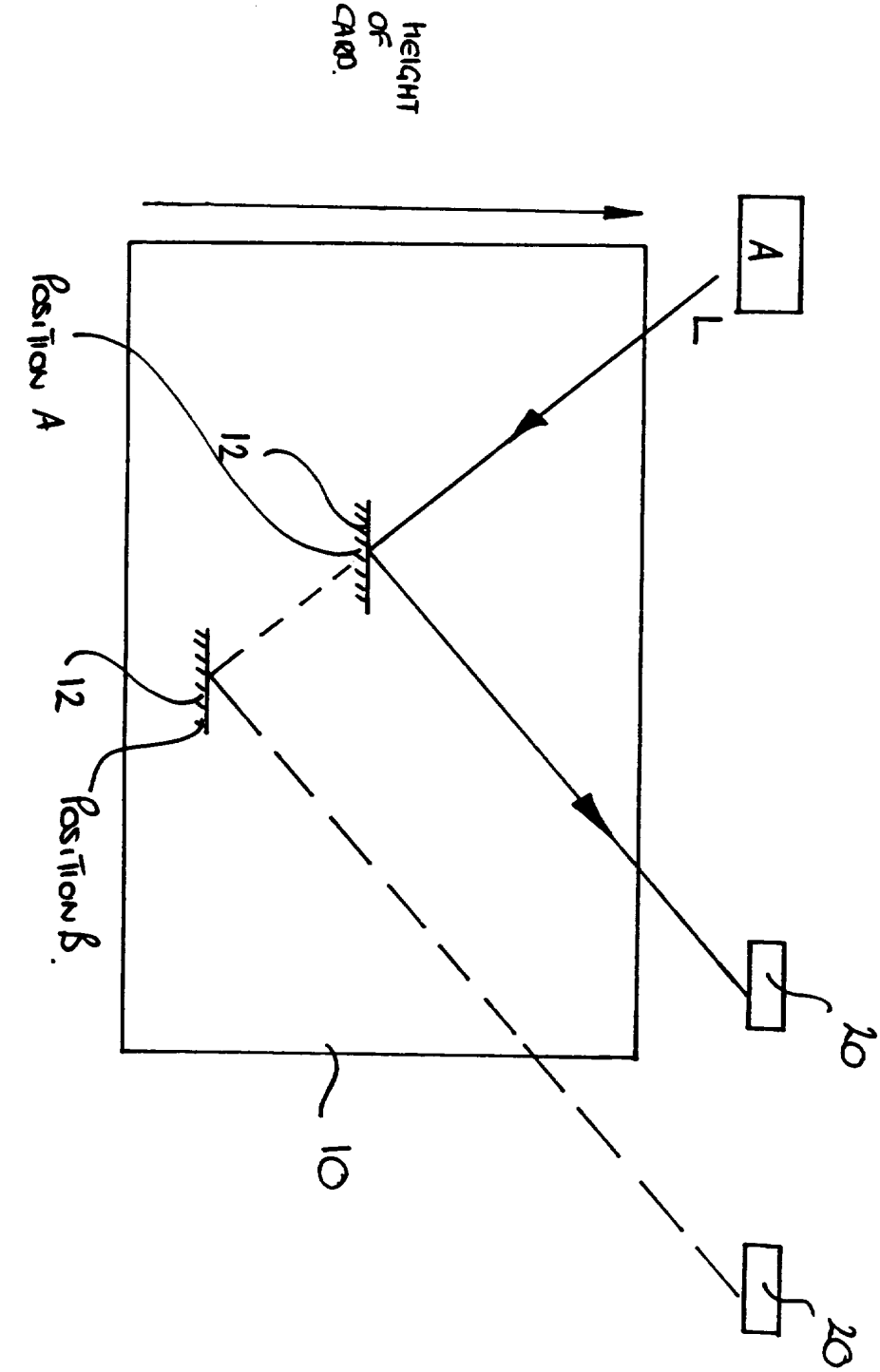


FIG 5

GB 2 304 077 A



CROSS SECTION OF CARD

FIG 1

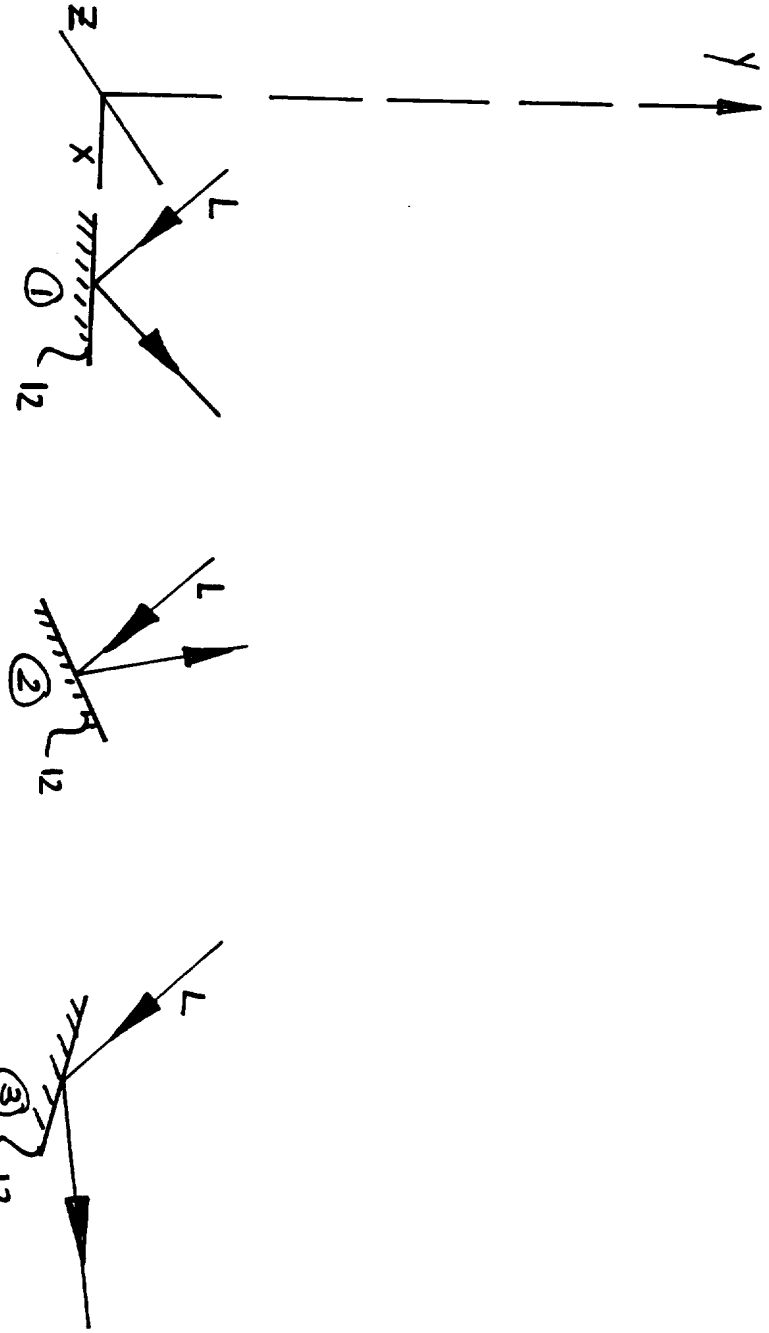


FIG 2

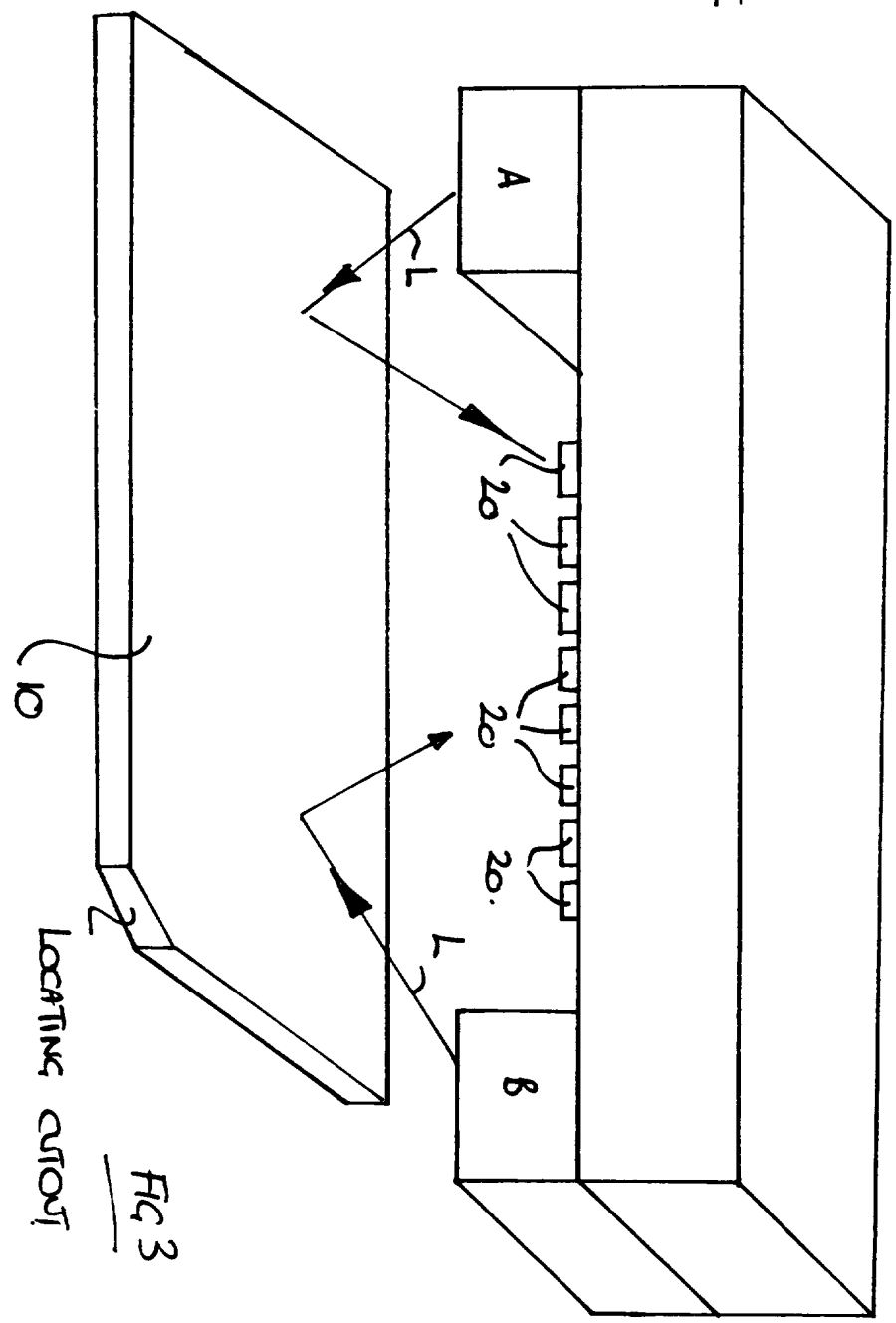


FIG 3

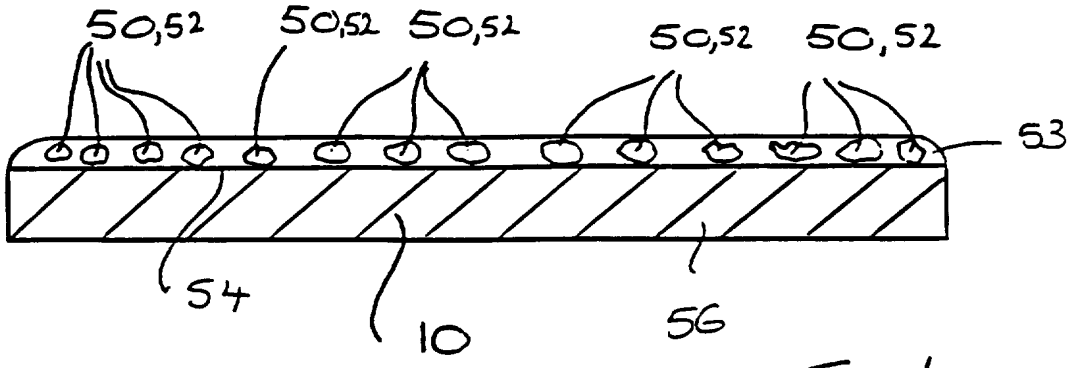

50,52
50,52
50,52
50,52
50,52
53
54
10
56

FIG 4

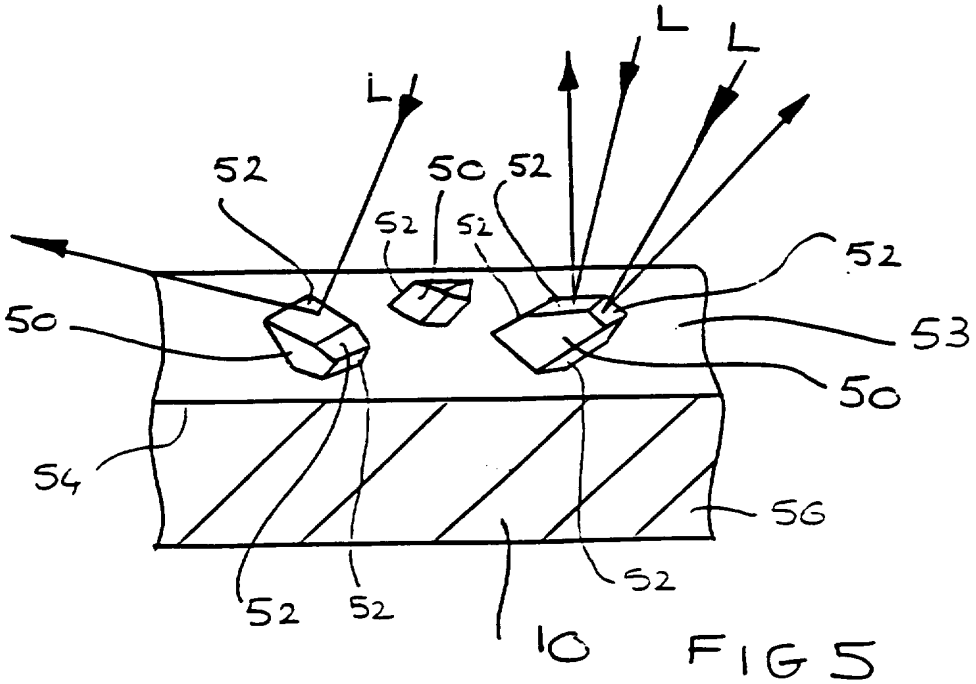

L
L
L
52
50
52
52
52
52
50
53
50
54
56
52
52
52
10

FIG 5

A SECURITY DEVICE

The present invention relates to a security device and relates particularly, but not exclusively, to such a device incorporating a plurality of reflective elements used to create a unique reflected light signature.

Most commercial security systems rely - to a greater or lesser extent - on security passes or identity cards of one kind or another. There are many types in use, from identity cards controlling physical access by specified personnel, to credit cards allowing cash to be drawn from a specified bank account. If even a single card is illegally duplicated then, at best, the security of the system will be compromised and, at worst, the system will fail completely.

Of course, modern identity cards carry numerous devices designed to make duplication very difficult. These range from photographs of the authorised holder, and laser-etched copies of the authorised signature, through to laser holograms attached to the surface of the card. However, it has to be said that such devices can only make duplication difficult, from a practical point of view they do not make it impossible.

It is an object of the present invention to provide a security device which reduces and possibly eliminates the disadvantages associated with the above-mentioned systems.

Accordingly, the present invention provides a security device or card having a unique and massive set of characteristics ("signatures") which - in practical terms - can never be duplicated.

In particular the present invention provides a security device comprising a plurality of reflective particles randomly distributed in three dimensions throughout a carrier material, said reflective particles in use acting to reflect light from a source thereof at a plurality of different angles and directions thereby to create a unique reflected light signature for detection by a signature reading device.

The present invention will now be more particularly described by way of example only with reference to the accompanying drawings, in which:

Figure 1 is a diagrammatic representation of a security device in accordance with the present invention;

Figure 2 is a graphic representation of the effect of rotation of the reflective particles in X/Y plane;

Figure 3 is illustrates the signature reading device which forms part of the present invention; and

Figures 4 and 5 are full and expanded cross sectional views respectively of a further embodiment of the present invention.

Consider a plastic card such as that used for credit or access control. Devices such as holograms and magnetic stripes attached to the card are man-made; hence, by logical extension, they are capable of duplication by man. The present device 10, on the other hand, relies on a signature set derived from a totally random feature - the presence of shiny metallic particles 12 randomly distributed in three dimensions throughout the very fabric of the device which is conveniently illustrated in the form of a card. When light L, in the form of narrow beams, is shone through the card 10 it may, or may not, be reflected depending upon whether or not it strikes a metal particle 12.

Random distribution of the metal particles 12 is achieved by stirring them into the bulk plastic material during manufacture, and before any individual cards are moulded or cut out. Hence the final position of any given particle inside any given card is defined purely by chance.

A number of anti-fraud systems have already been proposed which rely on reflective material of some kind embedded within the fabric of the card. The present invention, as explained below, is a radical new departure because it reacts not just to the presence (or absence) of reflective particles but also to the spatial orientation of each individual particle.

If metallic particles 12 in the form of thin flakes, rather than (say) spheroids, are used as reflectors then two distinct *random* factors come into play: the

distribution of the flakes within the fabric of the card, and the orientations of those flakes with respect to the card boundaries. Orientation within the card 10 is vitally important because the angle at which any light L is reflected will depend upon both the angle at which the light strikes the card and the angle at which the particle is laying inside the card. The effect of orientation in just one dimension is shown schematically in Figure 2. (The importance of orientation will become apparent when we discuss the way in which a card signature is decoded.)

Anybody attempting to duplicate a card made by the Crystal Chip process faces the problem of duplicating the exact individual distribution - and orientation - of possibly hundreds of minute metal fragments. If even one fragment is out of position, or incorrectly rotated, then the fraudster runs the risk of the fake being detected because one flake out of alignment may mean the card giving the wrong "response" when scanned by the security system.

Before going on to discuss how signatures are decoded it may be as well to look in a little more detail at the topic of flake distribution within the card fabric.

The following assumptions will be made:

1) that the card has external dimensions of 8.00cm x 5.00cm x 0.2cm (i.e. approximately credit card size, but a little thicker)

2) that each flake is laminar and 0.10cm square.

The maximum number of flakes possible across the horizontal (major) face of the card is given by the simple equation:

$$(8.00 \times 10) \times (5.00 \times 10) = 4{,}000 \text{ flakes}$$

It is, of course, theoretically possible to have many parallel horizontal layers of flakes distributed throughout the thickness of the card since the flakes are of negligible thickness, but for the purposes of this "minimal" analysis those additional flakes will be ignored.

So, if one major face of the card can contain 4,000 flakes then it follows

that both major faces could contain a total of 8,000 flakes. Ignoring the flakes held deep inside the card, and assuming that the card only holds approximately 5% of the theoretical maximum it follows that a card can easily hold some 300 - 400 flakes randomly distributed throughout its length, breadth and thickness.

The counterfeiter is faced with the task of duplicating the position and orientation of these 300 - 400 tiny flakes if he is to make an accurate copy of the card capable of analysis by the security system, i.e. signature decoding.

To decode the signature the card is placed in a series of narrow light beams which strike the card at an acute angle. If a beam hits a flake then it will be reflected and detected by one of a number of photoelectric cells 20 positioned in a group above the card. These "hits" are used to specify the card's signature, and can be recorded in binary form with (say) a miss being 0 and a hit being 1. The system shown in Figure 3 is just one example of how the signature of a card can be interrogated; factors such as the positioning of lights and photodetectors can be arranged to suit particular system requirements.

The factors controlling which photodetector is hit by which light beam are numerous (an obvious one is the positioning of the light sources with regards to the detectors) but, as was explained above, there are two totally independent factors which result directly from the card's structure - the depth of each flake under the surface of the card, and the respective orientations of these flakes.

Depth in the flake
Consider Figure 1. Assume that a beam is striking the card at an acute angle. If the flake is just under, yet parallel to, the surface of the card [*Position "A"*] then the beam will be reflected away and - in accordance with the laws of physics - the angle of reflection will equal the angle of incidence.

Now consider the case where the flake is some distance under the surface of the card but still parallel to the surface [*Position "B"*]. As before the angle of reflection will equal the angle of incidence, but geometry dictates that the beam will emerge from the card at a point further along the card's surface. If the group of detectors is kept small in relation to the dimensions of the card then the beam reflected from Position "A" will hit a different detector to the beam reflected from Position "B".

NOTE: For the purposes of this analysis any possible effects due to refraction at the card/ air boundary have been ignored.

Orientation of the flake
This is a primary factor in determining the signature set of any given card. As Figure 2 demonstrates, the incident beam can be reflected in any direction, not only away from the light source but even towards it. In other words, a beam entering the card through the top surface can exit from virtually any point on any surface of that card.

Reference has been made to any one card having a number of signatures. This arises from the fact that the card can be illuminated at different angles, from different light sources, and from different positions (e.g. first from the front, then from the side). Altering the source of light, or altering the angle of illumination relative to the card, will generate a different set of reflected beams and hence a different signature.

Most importantly, note that moving (or rotating) the light source(s) will mean that a **different** set of reflectors will be illuminated because the light beams will enter the card at a new angle(s) and at a new point(s) on the card surface.
This means that a counterfeiter trying to copy a card which will be scanned in two or more ways by the security system has no option but to try and accurately duplicate the position (in three dimensions) **and** the rotation (in three dimensions) of maybe 400 reflective particles. He cannot afford to ignore any reflector because he has no way of knowing which reflectors will be scanned by the system.

NOTE: The signature decoded by the system is a function of the system, NOT of the card.

Any given card contains a large (if not infinite) set of passive random signatures. The particular signature detected at any given time can be changed very simply by, for example:

- changing the layout of the beams and sensors,

- by scanning the card from a different direction,

- by scanning the card from a different angle, or

- by changing the order in which the sensors are interrogated.

As has been demonstrated above, the number of detectable signatures in a card is a function both of the number of narrow beams used to illuminate the card and the number of detectors used to identify the reflected beams.

Mathematically the signature can be expressed as the selection of sensors illuminated by the card's reflectors taken from the total number of sensors available in the decoder.

For example; consider an arrangement whereby the card is illuminated using the arrangement shown in Figure 3. [*Note that this is just an example arrangement - the layout of sensors/ light sources can be changed to meet individual system requirements*]. Light source "A" contains 5 independently rotatable lights shining down from left to right, and light source "B" similarly contains 5 independently rotatable lights beaming down from right to left.

The reflected beams are detected by a bank of 50 photodetectors arranged as a 10x5 matrix positioned between the light sources. The signature of the card on this occasion is thus represented by a random selection of 10 sensors being activated by the card out of a total of 50 equally available sensors.

Expressed mathematically this choice is given by the expression:

$$nCr = \frac{n(n-1)(n-2).....[(n-r)+1]}{r!}$$

where n = total number of sensors available for illumination
r = actual number of sensors illuminated.

Inserting the figures for this example gives the result:

$$50\ [C]\ 10 = 10,272,278,170$$

which means that there are over *ten billion* different ways in which any ten sensors can be illuminated at random out of a group of 50.

Put another way, the odds against two cards having an identical signature are in excess of 1:5,000,000,000 (over 5 *billion* to one against).

From a practical engineering point of view it might be decided to use fewer light beams or sensors. If the above calculation is repeated using only 30 sensors (in an array of 6x5) illuminated by 10 beams the number of possible random combinations becomes:

30 [C] 10 = 30,045,015

Odds against any two cards having identical signatures are now some 15 million to one against.

The basic card is envisaged as a piece of transparent perspex 8.00cm long by 5.00cm wide by 0.2cm thick, with laminar 0.10cm square fragments of reflecting material dispersed randomly throughout the card material.

This, however, is a very simplistic model of the Crystal Chip card because the parameters can be changed in a wide variety of ways. For example:

1) depending upon the number and width of the light

beams the card can be made thinner, or made in a different shape entirely. The reflecting fragments could also be made smaller;

2) one face of the card could be overprinted with normal security information, such as the holder's photograph or card serial number, and the card then scanned through the opposite face;

3) magnetic striping could be applied to the card as an additional feature so as make it acceptable (for other purposes) to swipe card readers;
4) by systematically changing the configuration of the sensors, and/ or their interrogation order, and/ or the relative angles between card, lights and sensors, the designer can carry out an automatic "sweep" to identify forgeries. (The true card will generate a series of signatures as the system configuration changes: a forger may be able to duplicate *one* of those signatures, but he will never be able to duplicate the full series since that would require the building of an exact replica of the true card).

5) the card can be used in conjunction with other standard features such as PIN numbers and/ or passwords;

6) the raw binary information recording hits and misses can be encrypted before the result of the card's scan is transmitted to the central control.

Examples of the system in use

System I - industrial access control
In this case the cards are used in conjunction with the normal keypad/ PIN number system to relate personnel to the card held.

At the time of its issue a new card is "initialized" in that it is put through a master scanner held by the Security Manager (or his designated officer) and the result of this scan entered on the recipient's file in the security system computer.

Also held in this secure file is the recipient's PIN number or password (of a suitable arbitrary type and length), details of the area(s) to which access is authorised, and any other information which the Security Manager has deemed appropriate.

To access a controlled area the holder places the card in the scanner and keys in his PIN/ password on the scanner's keypad. The computer compares the card's signature with the password/ access details held on file and - if a match is found - permits access.

If the signature of the card used does not match the PIN keyed in then access will be denied. Similarly, if a correctly issued card is used to attempt access to the wrong area then, again, such access will be denied.

The card's ability to give more than one signature can be exploited by arranging for scanners for different areas to have different light/ sensor configurations. In such a case the new card would have to be "initialized" into the system using master scanners appropriate to each permitted area. Using multiple signatures in this way allows for a very high level of access control to be set up.

If it were felt that the link between the individual entry control points and the master computer were a security weakness then the signature generated by the card could be encrypted using normal electronic techniques prior to transmission to the master computer.

To facilitate ordinary security procedures the card could be printed on one side with normal details such as photograph, signature etc, and then be scanned from the other side.

System II - credit card system
The purpose of this system is to identify the card offered and to compare its Crystal signature with the cardholder details held on file.

As with the industrial system the card's signature is first established prior to issue and recorded on the system.

Each Automatic Teller Machine (ATM) would have the same sensor/ detector configuration fitted as standard so that the card was always read the same way. The signature derived from the card would be compared with the PIN code to confirm whether the card was the original or a forgery (a forgery would generate the wrong electronic signature). Once the validation checks were completed the transaction could continue in the normal way.

For this system to be effective the ATM would need to communicate with the bank's central computer in real-time to compare the signature/ PIN offered with the signature/ PIN held on file for that particular customer.

Since the card could also bear a magnetic strip it could carry other information, such as credit limits etc, required by the banking system.

System III - document identification
This system is aimed at the identification of valuable original documents such as wills, contracts etc.

Instead of a perspex card a thin transparent sheet of security plastic (see below) containing an encapsulated Crystal Chip is attached to the document by strong adhesive. The idea is that during production this sheet's Chip - the "document tag" - is initialized by a standardised scanner and the decoded identity is printed on the tag in the form of a visible, indelible, unique reference number. This number is obtained by converting the binary output from the detectors (the register of "hits" and "misses") into a series of numbers and/ or letters using an agreed pre-determined protocol.

The transparent plastic sheet encapsulating the Crystal Chip has an adhesive lower face and contains two chemicals separated by a thin membrane. If the

sheet is subjected to mechanical stresses, such as cutting or twisting, the membrane will rupture allowing the two chemicals to react together. These chemicals are chosen so that a permanent irreversible reaction will occur causing the immediate formation of an opaque layer blanking out both the face of the tag and its border. Not only is the tag rendered useless but it becomes immediately obvious that it has been attacked.
When the document is ready for signing etc. a clause is inserted to the effect that the original "*.... is identified by the attached document tag, serial number* ****** ". In the presence of witnesses that tag is then permanently affixed to the document ensuring that the adhesive transparent sheet covers the clause identifying the tag number and the signatures of the witnesses.

A person attempting to forge a copy of the original would also have to forge the identity tag - which is a practical impossibility. Realistically his only options are either to transfer the tag from the original to the forgery, or to affix another tag. However:

- transference is thwarted by the fact that the original and its tag are permanently bonded together: separating them will - at best - rupture the security cover on the tag (so blacking it out) and may even destroy both components;

- affixing another tag to a forgery is not a viable alternative since each tag carries, permanently displayed on it, the unique reference number generated by its Crystal Chip capsule during manufacture. The number of the original tag will be shown on the original document and will not match that permanently displayed on the new tag. If, as a matter of routine, a controlled (and protected) record is kept of original documents and their tag numbers then undetected substitution of a second tag should be impossible.

System IV - passport/ ID card identification
This is an enhanced version of System III designed to deal with the special problems associated with detecting forged passports, national ID cards, vehicle documents and so on.

During its manufacture the original document is overlaid with a Crystal Chip tag which has been constructed and labelled as in System III. The reference number of the tag is printed onto the document prior to the tag being overlaid, and the tag is positioned so as to cover that printed number.

Since the document may be examined at any time by any authorised official it is essential that the generation of the tag number, and the official inspection of the tag when it is in place, are carried out according to an agreed national (or international) protocol. It is vital that standards are laid down covering such matters as:

- the conversion of the tag's binary output into its unique reference number, and;

- the configuration of the lights and photodetectors in the scanner.

To ensure that the document is correctly aligned in the scanner prior to examination the document would have two or more holes drilled in it by which it would be held accurately in place in the scanner during examination. The configuration/ placing of these holes would again be governed by an agreed protocol.

It is envisaged that the scanner used in this system would be based broadly upon that shown in Figure 3, but with the following additional features:

1) be hand held in use
2) be totally portable
3) contain suitable electronic systems to decode the signature
4) contain an integral screen, similar to that on a pocket calculator, on which would be shown the detected signature in the form of a numeric, or alphanumeric, display.

Having obtained a readout from the scanner the official would compare that readout with the printed tag number shown on the document. If they do not match then the document would immediately be treated as suspect and the necessary enquiries would be carried out.

It is assumed that a competent forger making (say) a complete passport, rather than modifying an existing real one, would apply a Crystal Chip tag whose number matched that of his forgery.

However, as a matter of course, documents such as passports and identity cards carry an ordinary sequential serial number. Comparing that serial number with both the name of the authorised holder *and* the number of the tag originally issued would quickly reveal a forgery. Either the serial number would not match the authorised holder, or the serial number would not match the tag number.

For the system to work as described above it would be necessary to record details of the authorised passport holder, the passport serial number, and the passport tag number on a secure computerised database which could be quickly accessed by the official carrying out the check. Setting up such a system would be both cheap and simple.

The system described above could be used to protect a range of official documents including:

- passports
- identity cards
- vehicle MoT test certificates
- driving licences
- vehicle excise licences
- high value theatre tickets
- gift vouchers
- banknotes
- cheques.

System V - counterfeit goods protection

This is another variation of System III designed to protect high value goods from the threat of counterfeiting.

In this process the Chip manufacturer mass produces small Crystal Chips which are overprinted during manufacture with their unique signature numbers (derived using a standardised process). The signature is displayed both as a printed number (or combination of letters and numbers) **and** as a barcode. Batches of Chips are then sold on to approved manufacturers of videos, CDs, high value aircraft components, high value electrical goods, etc.

By selling only to approved manufacturers access to the Chips can be carefully controlled, thus ensuring they do not fall into the hands of counterfeiters.

The approved manufacturers then attach a Chip to each item they produce, while at the same time, by means of the barcode, keeping a secure record of the Chip numbers assigned to each individual item.

Should a product be suspected of being counterfeit it would be a simple matter to scan the Chip and then compare the derived signature with the supposed manufacturer's records.

Note that the check is done by scanning the Chip itself: barcodes may be forged, but the Chip's true signature cannot be altered.

Turning now to figures 4 and 5, from which it will be appreciated that the present invention could make use of three dimensional granules 50 of reflective material (rather than flakes) in which each granule comprises a plurality of randomly distributed and orientated reflective surfaces 52. These surfaces may be employed in much the same way as those described above but, as each granule 50 comprises a plurality of reflective surfaces 52, each granule can provide a plurality of reflected light beams for creation of a significantly more complex "signature". Each granule can be as small as 100 microns in diameter and still provide a unique and identifiable reflection. Such a granular arrangement may employ granules 50 in the body of the security device itself or in a transparent coating 53 applied to the security device. Indeed, the coating may even comprise the security device itself and may be applied to, for example, an aircraft component requiring a unique identification marking. Clearly, the flake arrangement might also be employed in this manner. the granules 50 may be held in suspension in the coating or applied to the surface 54 of a base 56 before a protective coating is applied. When applied to the base 56, one or other of the reflective surfaces 54 will tend to act as a bottom surface 58 securely locating the particle itself. In practice, it will be appreciated that the protective coating and granules 50 may be mixed together and applied to a surface of an object or the security device in much the same way as one would apply paint to a surface.

Further to the above, it will be appreciated that the protective coating 53 need not be visually transparent as on e could employ materials transparent only to infra red or ultra violet or other wavelengths of light.

Counterfeiting of the granular based system is considerably more difficult than the flake based system as it is necessary to replicate the position of each granule and the angular orientation of a plurality of randomly distributed reflective surfaces provided thereon. For all practical purposes, such replication is impossible.

For the purpose of a multi-level security device, one could interrogate the granules from a number of different angles, each angle creating a unique "signature". Such an arrangement could be employed when a user is entitled to have access to one restricted area but must be denied access to other, more sensitive, areas.

CLAIMS

1/ A security device comprising a plurality of reflective particles randomly distributed in three dimensions throughout a carrier material, said reflective particles in use acting to reflect light from a source thereof at a plurality of different angles and directions thereby to create a unique reflected light signature for detection by a signature reading device.

2/ A security device as claimed in claim 1 in which the reflective particles comprise flakes of reflective material.

3/ A security device as claimed in claim 1 in which the reflective particles comprise three dimensional granular elements having a plurality of randomly distributed and orientated surfaces provided thereon.

4/ A security device as claimed in any one of claims 1 to 3 in which said reflective particles form an integral part of the carrier.

5/ A security device as claimed in any one of claims 1 to 4 in which the security device comprises the carrier material and reflective particles themselves.

6/ A security device as claimed in any one of claiims 1 to 5 in which said device comprises a credit card, an identity card , an identity tag or identity label.

7/ A security device as claimed in any one of claims 1 to 6 in which said reflective particles are randomly distributed throughout the entire body of the security device.

8/ A security device as claimed in any one of claims 1 to 7 including means for presenting further security information on a surface of the device itself.

9/ A security device as claimed in any one of claims 1 to 8 including a magnetically stored PIN number or password.

10/ A security device as claimed in any one of claims 1 to 9 when manufactured by mixing the reflective particles into the buik of material used to form said device and then forming said device with said particles embedded therein.

11/ A security device as claimed in any one of claims 1 to 10 further including a signature reading device comprising a light source for directing light onto a surface of the device, light detector means for detecting the presence or absence of reflected light at a plurality of points adjacent the device and means for decoding a signal generated by said detectors thereby to create an electric signal for subsequent use in an automatic identification procedure.

12/ A security device as claimed in claim11 in which said signature reading device includes a plurality of photo detectors positioned in a matrix formation and configured for creating a binary coded signal upon being hit or nissed by reflected light.

13/ A security device substantially as described herein with reference to and as illustrated in the accompanying drawings.

The Patent Office

16

Application No: GB 9525734.1 **Examiner:** Graham Russell
Claims searched: 1-13 **Date of search:** 25 April 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): B6A (ATC)

Int Cl (Ed.6): B42D 15/00, 15/10; G06K19/06, 19/14; G07F 7/08

Other: Online: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 0570162 A2	(CANON) see column 3 line 20 - column 5 line 17	1,11
X	EP 0388713 A2	(UNILEVER) see aluminium particles 6 and WPI Abstract accession No 90-092375/13	1,6
A	EP 0364029 A1	(HOMER) see column 5 lines 19-33	1,11
X	EP 0230497 A1	(MAURER) see reflecting aluminium particles and WPI Abstract accession No 87-214936/31	1,6
A	US 4423415	(LIGHT SIGNATURES) see column 5 lines 22-37	1,11
A	US 4218674	(DASY) see column 7 lines 8-26	1,11

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.